● 作者/Amy Zegart and Michael Morell ● 譯者/章昌文 ● 審者/馬浩翔

新型態情報戰

Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail

取材/2019年5-6月美國外交事務雙月刊(*Foreign Affairs*, May-June/2019)

面對世局詭譎多變與科技的快速進步，單靠以往傳統情報蒐集方式與應變作為，已不足以維護國家安全，因為新科技已改變情報戰的形態。因此，美國須訂定能因應當前世界變化的情報戰略，才能立於不敗之地。

九一一事件促使美國國家情報體系進行改革。(Source: Wiki)

對美國情報機關來說，二十一世紀在震驚中展開，當時19名蓋達組織的恐怖分子劫持四架飛機，並在美國本土上犯下最致命的攻擊。攻擊發生後，情報界全面動員，只為了一個凌駕一切的目標：阻止再次發生九一一恐攻事件。美國中央情報局、美國國家安全局和美國情報界內的15個單位進行結構重組、改革及重新購置設備，國會撥款數十億美元來支持該項轉型。

努力也確實奏效，在美國情報機關專心對付恐怖分子的近二十年來，他們阻止了無數次攻擊美國本土的陰謀、搜獲賓拉登、協助剷平自稱為哈里發的伊斯蘭國、從阿富汗的洞穴到布魯塞爾公寓大樓中找出藏在各處的恐怖分子，這被視為是美國情報史上最成功的一個時期。

今日要對抗的新威脅遠不只是恐怖主義，美國情報機關正面對另一次的評估時刻。從生物技術、奈米技術，乃至量子計算和人工智慧，快速的技術變遷使美國敵人具備新能力，也削弱傳統的美國情報優勢，美國情報界必須適應這些轉變，否則恐承受國家第一道防線失效的風險。

儘管美國情報機關已往正確方向邁出去了，但進展仍不夠快，實際上，此新時代的第一次情報失效已經發生：無法全盤快速掌握俄國使用社群媒體干預美國2016年總統大選的程度。這次失誤應視為是個警訊，其反映出有必要大刀闊斧重新檢視情報界的運作情形。要做到這點，將需要充分利用美國獨特的優勢，並做出艱難的組織變革，同時重新取得美國科技公司的信任。

一個警訊

俄國在美國2016年總統大選前採取多面向「積極措施」的行動，旨在削弱民眾對美國民主程序的信心、激起美國社會的分歧，以及煽動民眾偏好支持某位總統候選人。這些作為並非大多都是在檯面下進行，像是針對美國民主黨全國委員會及希拉蕊(Hillary Clinton)競選活動發動網攻，在維基解密(WikiLeaks)平臺與大眾共享偷來的資訊，試圖滲透全國與地方投票系統，好在美國情報機關幾乎

美國前特別檢察官穆勒(Robert Mueller)為其提出俄羅斯涉干預美國2016年大選之報告作證。穆勒於國會聽證中警告，俄國恐將再干預2020年的選舉。(Source: AP/達志)

立刻察覺到這些不法活動。鑑此，早在大選之前，情報官員就警告當時的歐巴馬總統，美國遭到了攻擊。

但美國情報機關卻錯過了俄國最重要的手段：社群媒體武器化，參議院情報委員會的委託研究與特別檢察官穆勒(Robert Mueller)對俄國「巨魔農場」(troll farm，譯者註：一個有組織的網路攻擊團體，他們利用大量假帳號在網上散播消息引導輿論，甚至編寫機器人對話程式與網友討論，讓目標中的話題標籤及關鍵字成為網上主流，從而引導民意)所提出的起訴，都凸顯社群媒體行動旨在動搖美國大選程序，且有可能早在2012年就已展開，到了2014年時就已進展得相當順利。儘管美國情報官員知道俄國曾用社群媒體的宣傳手法來對付自身國民及其鄰國(特別是烏克蘭)，但還是至少花了他們兩年時間，才意識到俄國對美國也在採取類似行動，此一疏失，使美國總統無法充分了解莫斯科之意圖，以及剝奪在大選尚未開始前擬定政策方案的寶貴時間。

2016年10月，在美國總統大選前一個月，美國國家情報總監克拉柏(James Clapper)與國土安全部部長詹森(Jeh Johnson)採取罕見措施，發布有關俄國介入美國大選的公開聲明，即便如此，美國情報人員卻依然未能掌握俄國的行動全貌，值得注意的是，該聲明對社群媒體未置一詞。好在詹森後來提到，俄國的社群媒體行動是「我們剛開始正視的……一些事情。」同樣地，克拉柏在其回憶錄中寫道，「在2015年夏季，我們還未曾想過低階俄國情報特工有可能在社群媒體上冒充美國人。」的確，直到大選過後許久，情報界還不清楚攻擊規模，該攻擊波及了1億2,000多萬美國公民，參議院情報委員會在2018年指出，美國情報界做的兩黨調查中，也是到了2017年才「揭露了更多俄國如何藉由操縱社群媒體管道煽動紛爭的事件，並且介入美國2016年總統大選及干擾美國社會等作為。」

美國情報機關有充分理由不將其蒐集系統針對其國內社群媒體內容，反觀俄國是由其國內民眾發動社群媒體攻擊。俄國在2014年派遣數名特工至美國，其明確目標是研究如何使俄國社群媒體活動更有效攻擊美國民主體制。克里姆林宮在競爭激烈的美國總統大選中是否發揮了決定性作用雖永遠難以得知。但可以確知的是，美情報人員對俄國惡意運用社群媒體的後知後覺，倘若情報界不能適應今日快速的技術突破，這項過失只不過是山雨欲來的前奏而已。

不可或缺的情報

情報一直是戰爭與治國之道的關鍵，中國軍事戰略家孫子在西元前500年左右就傳授了「知敵」。在戰場上，可靠情報能測定敵方兵力、預判其爾後之行動，並了解對手企圖、計畫及戰力，同時有助於拯救性命並贏得戰爭。在戰場下，透過預防誤判、以及能即時洞悉威脅與機會，情報能協助領導者做出更好的決策。例如在1962年，U-2間諜機蒐集的情報，使甘迺迪總統有時間與證據，無須觸發核子戰爭就迫使蘇聯從古巴移走核武。當然，情報也可能會出錯，有時甚至錯得離譜，一如

伊拉克戰爭前對海珊大規模毀滅性武器計畫的評估。情報在本質上就是不確定的事務，涉及拼湊敵人存心否認與欺瞞的片段資訊。

但情報歷久不衰的價值來自一個基本事實：當政府領導人有更好資訊時會做出更佳決定，而美國情報機關長久以來都能較其他來源提供更佳資訊。透過人員特務和技術方式，他們蒐集敵人試圖隱藏的祕密資訊，並將那些機密跟來自政府其他部門的資料，以及從新聞報導、非機密外國政府文件和公開聲明等公開性資訊(這僅是列舉其中一小部分)整合在一起，他們為決策者的特殊需求量身打造，並在不參雜個人意見、黨派偏私或政策議程的前提下將其呈報。

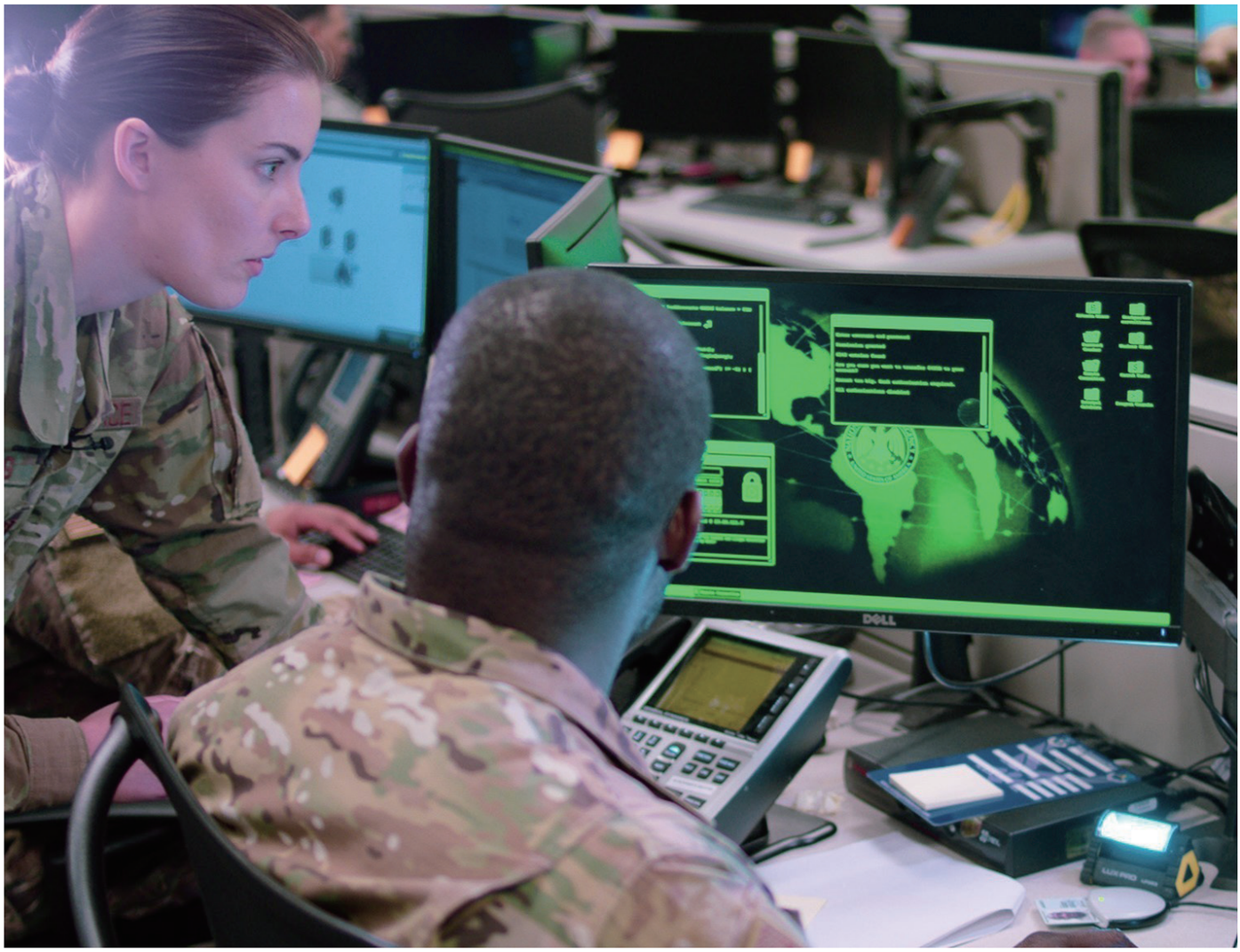
目前雖對這些能力需求甚殷，但新威脅和新技術使得情報蒐集與分析較諸冷戰初期以來任何一刻都更具挑戰性。近期由國家情報總監辦公室所發布的年度威脅評估報告，描繪出令人頭暈目眩的全球風險圖像：崛起強權的競爭，特別是來自中共和俄國；北韓及印巴邊界日益增加的核子火藥庫；紛亂不堪的中東孕育出極端主義；日漸崩壞的國際秩序；獨裁者正從歐洲往亞洲推進。另氣候變遷迫使無數人離鄉背井，更加劇了現有的不穩定。「灰色地帶」衝突和「小綠人」(little green men，譯註：在烏克蘭危機中，穿著無標誌綠色軍裝卻攜帶俄製現代武器裝備的人)模糊了戰爭與和平間的界線，即便戰鬥也已非舊有面貌。

於此同時，美國情報機關正面對突破性技術所產生的新挑戰，2007年，年度情報威脅評估報告中尚未出現過「網路」一詞。2009年，此詞夾藏在共45頁文件中的第38頁，就在西非毒品走私的下一段。而到了2012年，僅僅三年後，時任美國國防部部長潘尼達(Leon Panetta)警告，一場「網路珍珠港」有可能無預警摧毀美國的關鍵基礎設施。現今，每天都有各式各樣的惡意行為者在全世界發動數以百萬計的網路攻擊，網路犯罪現在產生的收益，比全球非法毒品交易更豐厚。

在新技術、威脅數量激增、複雜性及威脅速度等交互作用下，這意味著美國處在更危險的情況，所以對其情報機關的要求也會來得高。例如，試想一下美國攻勢網路行動這個新興領域，在實體世界中，許多軍事目標是不會移動的建築物，因此目標清單與作戰計畫有期限，計畫參謀可以確定一枚威力十足炸彈可將爆炸半徑內的任何建築物夷為平地，無論它有多少窗戶，多少水泥或木造的牆壁。但在網路空間中並非如此，裡面的目標是不斷在改變的機器或系統，即使只對某一目標做細微修改(諸如安裝一個簡單的修補程式)，都可能讓對付它的網路武器完全失能，同時不斷轉變的樣貌，也讓攻擊的附帶損害難以預測。因此，目標清單需要即時更新以隨時可用，今日情報不只是媒介，如同前國家安全局副局長殷格里斯(Chris Inglis)近期所寫的，情報是有效行動的一個「關鍵述語」。

公開的祕密

技術進步往往對情報而言是把雙面刃，幾乎任何的技術發展都可使敵人能力更強並削弱現有防禦。但這同時也可讓情報機關更好也更快完成工作。例如，人工智慧雖可改善分析，但也讓人



「網路珍珠港」的破壞力難以想像，情報界須加快應對網路攻擊的挑戰。(Source: USAF/Christopher Vasquez)

幾乎無法偵測敵人發動的資訊戰，商用加密服務雖保障美國公民與決策者的通信，卻也讓恐怖分子能夠密謀行事。人工智慧、臉孔辨識及生物統計學等技術，可以幫助機構逮住通緝犯，但它們也提高了傳統祕密行動的困難度。

有愈來愈多智慧型裝置連結到網際網路，結果造成公開資訊激增，這也充分說明了新技術具有雙面刃之特性。目前世界上有超過半數人口在上網，照粗略估算，明年有手機的人會比有自來水可用的人還多，此種連接性正將一般公民轉變成刻意為之或無心插柳的情蒐員。手機可錄製事件，甚至可即

時記錄地下核子試驗之類影響深遠的活動，監視器拍攝全世界城市所發生的大部分事情，社群媒體、搜尋引擎及線上零售平臺揭露大量用戶資訊。對分析家來說，這是個豐富的資訊寶庫。祕密依舊重要，但公開資訊已變得更無處不在，並具有潛在的價值，對敵我來說都是如此。

公開資訊甚至有辦法接觸到祕密不易滲透的領域，俄國在2014年入侵烏克蘭東部時，最具說服力的證據來自俄國士兵所拍攝有時間標記，並張貼在社群媒體上的照片，因為背景就是戰車運輸車和烏克蘭高速公路的標誌。同樣地，就在馬來西亞航空17號班機遭擊落前，社群媒體拍攝到俄國先進SA-11防空系統如何運送到烏克蘭東部，以及後來如何運回俄國。社群媒體變成如此珍貴的資源，也讓美國戰略司令部地下核子指揮中心的控制臺場景，隨著推特的推文而揭露內部的設施。

於此同時，容易取用的資料與技術，更是讓美國情報界付出許多代價。更多國家，包括如伊朗和北韓及非國家行為者等美國的敵人，現在都能以極低代價在全世界蒐集情報。任何上網的人，都可看到谷歌地圖上的圖像、追蹤推特上的推文，並以臉孔辨識軟體在網路挖寶。2011年當美海軍海豹部隊突襲賓拉登在巴基斯坦的居處時，巴國軍隊並未偵測到該次行動——但當地一名叫艾薩爾(Sohaib Athar)的資訊技術顧問卻察覺到了，當美軍部隊著陸時，艾薩爾開始在推特上發文，表示聽見不尋常噪音，他寫道，「直升機凌晨一點在亞波特巴德(Abbottabad)上空盤旋，這可是件新鮮事」，艾薩爾繼續在不知情情況下推文描述該突襲，甚至提到某次爆炸震動了他家窗戶，不難想像類似情況未來會如何使美國行動陷入險境。

商用衛星目前為所有有心者在天空提供廉價的眼睛，直到約十年前，美國和俄國以幾個尺寸約公車大小的大型間諜衛星掌控太空市場，每個設計與發射費用須花費數十億美元，使用極其先進的技術，蒐集機密資訊。中共現在已加入此菁英團體，但急遽下降的發射成本、更強大的商用光學技術及體積縮小，讓太空技術獲得更廣泛運用。過去五年間，擁有及操作衛星的國家數目已加倍成長，年度發射次數增加了400%。2018年12月，SpaceX航

太公司發射了一枚火箭，內建來自17個國家的64枚小型衛星，這些衛星價格不高、約鞋盒大小，可為全球付費用戶提供影像與分析資料，儘管仍比不上美國政府的衛星，但這些衛星正在日益精進中。

欺敵革命

美國情報界必須弄清楚如何比敵人更快、更善加利用資訊公開優勢與各式技術，同時此項作為必須在憲法與道德義務間取得平衡，以保障隱私及公民自由。

這事知易行難，再次細想公開來源資料的情況，中世紀時紙張是財富的象徵，而書本鎖在修道院中，知識寶貴且創造知識所費不貲。現在，創造內容是如此廉價，根據估算，存放在地球上的資料量每兩年會成長一倍，這意味著人類在未來24個月就會產出相當於人類歷史迄今所產出的資料量，情報機關總得在乾草堆中找出針來，而如今乾草堆正大幅增長。

許多民營公司正採用「社群聆聽」(social listening)和其他解決辦法，亦即善用並快速存取公開來源資訊。隸屬中央情報局的In-Q-Tel風險投資公司，以創業基金培養過許多前景看好的技術新創事業，要讓任一技術創新在情報機關內生根都會是一項挑戰，因為合作廠商會有其自身收益考量，另量身打造且過時的資訊技術系統，以及僵硬且規避風險的招標作法，也讓民間公司，特別是新創事業極難與政府合作。

蒐集與處理資料不過是戰爭的上半場，除非分析師能評估資訊可信與否，否則再多資訊亦無多大用處。當事涉祕密情報時，可信度絕對是一項挑戰，這在公開來源的世界中甚至是個更大的問題。部落客、公民記者及其他線上內容提供者出自不同動機而發文，重視的是速度和煽動性，而不是準確無誤，因此，出錯的風險極大。

雪上加霜的是，日漸增長的時效挑戰，在谷歌時代中，僅需敲打或按個鍵，任何人都能針對任何事提供資料，公開來源內容不需經審查或分析，就能直接源源不絕流入決策者手中，這讓決策者不去等候慢工細活、經深思熟慮其來源可信度，以及對突破性發展提供更多詮釋的情報判斷，反而增加了做出倉促判斷的風險。為了要跟上這個環境，情報分析師被迫加速動作，有時得放棄追根究柢作為代價，與公開來源資訊競爭也有可能加重分析師壓力，使他們被迫製作短期情報分析，而不是一些早已短缺的長期且超水準分析。

分辨真假只會變得更難，人工智慧正在引發欺敵革命，不久即有可能成真的深度偽造(以數位操縱影音資料，並盡可能仿真)，其效果驚人，而俄國在2016年大選前的假情報實在難以比擬。商業與學術研究員早就為不存在的人創造出極其逼真的相片，史丹福大學和華盛頓大學的共同研究小組分別透過人工智慧和對嘴技術，在深偽影片中讓歐巴馬說出他從未說過的話。和其他技術一樣，人們有愈來愈多機會可使用簡化的深偽碼，有些程式簡單到能讓那些就算不具電腦科學背景的高中生，都可透過技術產出令人深信不疑的贗品，甚至那些能製造檔次更高深偽造效果的高階電腦，現在也可用相對較低的價格獲得。

深偽影片是假新聞的最新形式，後續影響力不容小覷。圖為川普合成影星尼可拉斯凱吉(Nicolas Cage)的有趣深偽影片範例。(Source: deepfakesweb.com)

此項技術的操縱潛力不證自明，想像觀看一部看似真實的影片，片中某位外國領袖意欲建立祕密核子武器計畫，或在大選前幾日，指控某位總統候選人性騷擾孩童，當事人即便矢口否認卻仍然無力回天，因為證據看來不容置疑，畢竟眼見為憑。

情報機關將要面對揭露深偽技術這項艱鉅任務，而不同於其他竄改圖像之類的　品，深度偽造格外難以察覺，因為有名谷歌工程師在2014年運用了人工智慧技術發明「生成對抗網路」(generative adversarial networks)：其讓兩部電腦的運算法彼此拮抗，一部產生圖像，另一部則試圖挑出偽冒圖像。因為該演算法是透過彼此競爭學習，而深偽偵測器在技術成熟前恐怕不會發揮太大作用。欺敵一直是諜報和戰爭的一部分，但不曾有過這種程度的精準、等級與速度。

確保戰略正確

美國情報界已採取了一些重要步驟，來適應此種快速變動的技術環境。2015年，中央情報局局長布瑞南(John Brennan)創立一個新部門，著重在數位創意及改革中央情報局體系，部分也是為了將數位專家和公開來源情報官員，跟中央情報局的傳統情蒐人員及分析師更緊密聚在一起。美國國家地理空間情報局(National Geospatial-Intelligence Agency)已開始一項人工智慧方案，期加速並改善影像分析。中央情報局、國家安全局及其他機關已往雲端系統發展，創建了一個「大數據整合環境」，這讓分析師能夠更快、更有效查詢大量數據。至於其他許多改進仍在保密中。

這些雖都是前景看好的作為，但個別修正仍嫌不足，在新科技時代中，情報界需要有整體的戰略，來重新獲得並維持國家的情報優勢，2019年〈國家情報戰略〉報告遠未達此一目標，卻明顯表達出自以為是的口吻，還提出了語意不明的告誡，如「增強整合與協調」、「更妥善運用夥伴關係」及「在保障國家安全資訊同時提升透明度」。創新被貶謫到只剩半頁。

一套能合乎新技術時代的國家情報戰略，應是找出美國的獨特強項，並善用這些強項來確保長期優勢。現今多數外交政策探討，卻都著重在美國的弱點上，描繪出的是一國被無情且效率高的獨裁者孤立、掀開弱點且超越的景象。一套新情報戰略應出奇招，起點應是了解何為美國擁有其他競爭者難

以匹敵的部分，以及這些能力如何能彌補各項弱點，而非屈從對極權的嫉妒。

美國在許多領域都勝過其敵人。眾多盟友——包括與澳大利亞、加拿大、紐西蘭和英國建立的五眼聯盟(Five Eyes intelligence partnership)，擴展了美國的全球影響範圍與能力，人民種族的多樣性在蒐集全球人類情報上具有先天優勢，美國的開放社會和民主價值觀，長久以來都在鼓勵想法的自由傳播，並幫助說服其他外國及個人加入其大業，而美國的創新生態系統，持續成為突破性技術無可匹敵的育成中心。

不過要善用這些強項，將需要全體情報界的努力，再加上來自技術公司、公民社群及學術界的參與。一個由國會建立與監督的藍帶委員會，可以推動此項改變，雖無法預測此程序會產生何種想法與倡議，但顯然已有幾個重點領域。

在組織方面，須有單一機構處理公開來源情報，目前情報蒐集是透過中央情報局的公開來源機構(Open Source Enterprise)去執行，但此安排有如將空軍限制在陸軍內部，把一項新任務擺在一個偏好其他優先事項的官僚體系內加以約束。由於機密在中央情報局依舊佔有絕大優勢，所以公開來源資訊就只能淪為次級品。只要公開來源情報仍歸屬於中央情報局或其底下的機構所管，就永遠得不到其所需關注與資金。

人力資源同樣重要，情報機關內現行雇用體

新科技時代中的美國國家情報戰略，應從他國無法匹敵的優勢出發，並由公私部門協力實踐戰略。(Source: Office of the DNI)

系是為不同時代所設計，當時的情報官員畢生擔任公職。現在在某些機關中，許多第一流員工在短短數年後就掛冠求去，帶走自身專長與訓練，一去不回。由於緩慢且官僚的徵募程序，有更多人甚至過其門而不入，尤其難吸引與留下技術專家。情報機關需要培養更多大使級人物，而非終身職員——引領政府內外的年輕和中年技術人員，來改善美國科技產業和情報界間的關係、理解與信任。

的確，消除科技產業和情報界間的隔閡，是國家安全的當務之急，對諸如蘋果、臉書、谷歌和其他科技巨擘來說，國防部前聘員史諾登(Edward Snowden)在2013年揭露的監控計畫，造成了官民間深刻且長遠的不信任感。推特因關心其資訊可能會遭濫用，不願與情報機關做生意。一家大型科技公司，同時身兼另一間頂尖科技廠商的前資深主管告訴本文作者之一，他們將美國情報機關看作等同於中共政府特工這類對手，不能讓其染指系統。

就情報機關而言，他們愈加擔憂美國科技公司願意將其產品和服務售予外國客戶，而這些外國人並未認同美國民主原則或國家利益。擁有某些世界上最頂尖人工智慧技術的谷歌，就曾表示他們不會與五角大廈在任何可用於製造武器的人工智慧專案上合作，但它卻在考慮幫助中共政府發展審查更仔細的搜尋引擎。俄國極力推崇的深度學習專案iPavlov，使用的硬體產自總部位於加州的業界頂尖公司輝達(NVIDIA)，該公司副總裁為了生意，近期公開表示，「我們將這些產品賣給每個人。」因應此種商業誘因、隱私與國家利益衝突，需要美國情報界和矽谷間營造更佳合作關係。

首要原則

就所有需要改變的事情來看，更重要的是甚麼該維持原樣，任何轉型作為的絕對優先項目，不應危及情報界中最有價值的資產：無論政策或政治如何作用，都維持對目標投入。此一原則說明為何世世代代的決策者都信任情報界的工作——這並非在某種意義上信任情報永遠是對的(並非如此)，而是在某種意義上相信沒有居心叵測的動機、政治議程或黨派價值在背後推動。

此一核心原則正遭到某位總統考驗，他公開貶斥其情報幕僚，且毫不隱諱地否定其機關評估，如此對情報界施壓，迫使他們「依照」總統的方式，而非依證據辦事。目前在國家情報總監柯茨(Dan Coats)指揮下，情報界雖仍能恪遵倫理，但冒著很大的風險。美國情報界能夠在新技術時代中發展最佳情報戰略，惟其一旦喪失客觀性、不偏好某黨及專業精神的名聲，將喪失對國家的價值。

作者簡介

Amy Zegart現任胡佛研究所、史丹福大學斯柏格里(Freeman Spogli)國際研究所高級研究員。

Michael Morell為美國中央情報局前副局長及代理局長，他目前擔任燈塔全球戰略諮詢公司地緣政治風險評估(Geopolitical Risk Practice at Beacon Global Strategies)全球主任。